**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**WASHINGTON, DC 20554**

**RE: ET Docket No. 15-170, RM-11673**

## COMMENTS OF MOZILLA

Mozilla is a nonprofit organization that produces the Firefox web browser and Firefox OS smartphone operating system, together adopted by half a billion individual Internet users around the world. Mozilla is a foundation that educates and empowers Internet users to be the Web's makers, not just its consumers. Finally, Mozilla is a global community of technologists, thinkers, and builders who work together to keep the Internet alive and accessible. Our mission is to promote openness, innovation, and opportunity on the Web.

Our products are produced and distributed as open source technologies, incorporating the contributions of others and offering code for use in downstream products by individuals, non-profit organizations, and for-profit corporations. This fundamental openness and freedom to tinker with technology reflects our mission, creates a global Web that is shaped by a diversity of views rather than a monolithic vision, and ultimately produces a more innovative and generative ecosystem with economic benefits for all.

From this perspective, we submit comments in this proceeding to highlight an area of possible concern: the future of open source software powered wireless devices.

We welcome the intentions behind this proceeding. Updating and modernizing the Commission's current licensing rules to reflect the increasing significance of software controls for radio devices[1] brings potential benefits for efficient spectrum use and thus more powerful

[1] *Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment; Request for the Allowance of Optional Electronic Labeling for Wireless*

wireless technologies. And recognizing where insufficiently flexible regulatory frameworks are impeding technology evolution and broad deployment is to be commended.[2]

In general, most of the proposals in the NPRM seem reasonable, and likely to produce a balanced framework to address the importance of promoting innovation and technology development, and protecting against interference and other harms from unlawful spectrum use. Testing equipment alone, without needing to use official facilities or register devices in a database, seems conducive to innovation while promoting rule compliance.[3] We appreciate the intention to allow for subsequent changes, so long as they would not modify wireless emissions in harmful ways, without requiring a new FCC ID.[4] And requiring a new certification when software would modify wireless operations to go beyond the originally approved RF parameters is similarly reasonable.[5]

However, the question of enforcement of these reasonable policy balances looms over this issue. In particular, some proposals in this NPRM and prior Commission documents indicate the possibility of technological locks on wireless devices that would impede the ability of software to modify wireless transmissions. The NPRM specifically "would require any RF device that uses software to control its defining parameters to incorporate software security features that permit only those parties that have been authorized by the manufacturer to make changes to the device's technical parameters."[6] Certification would require "devices incorporating software controls [to] address specific security requirements."[7] And certification

*Devices*, Notice of Proposed Rulemaking, FCC 15-92, ET Docket No. 15-170, RM-11673, para. 37 (*Wireless NPRM*).

[2] *Id.* at para. 45.

[3] *Id.* at para. 27.

[4] *Id.* at paras. 52-54.

[5] *Id.* at para. 72.

[6] *Id.* at para. 20.

[7] *Id.* at para. 22.

holders “must implement well-defined measures to ensure that certified equipment is not capable of operating with RF-controlling software for which it has not been approved.”[8]

These standards are not well specified, but as one example, past guidance from the Office of Engineering and Technology has encouraged applicants for equipment authorization to “describe in detail how the software is protected against modification.”[9] If the intention is to prevent all possibility of modification of all software that touches on wireless controls, then the potential ramifications are significant and severe.

These concerning provisions seem fundamentally incompatible with a modern day technology world that today is built largely on open source software. Tellingly, perhaps, the NPRM does not mention the phrase “open source” even once. The NPRM as written may properly befit a world where software that affects radio usage is written and distributed exclusively by manufacturers of radios and devices. But this isn’t always the case. The Commission must ensure that its rules reflect the modern wireless world and do not stifle open source technology development and use.

**The Commission’s rules must permit open source technology.**

As part of the technology evolution that this NPRM seeks to respond to, open source software powered wireless devices have become a marketplace reality. This universe includes but extends far beyond well-known examples like hobbyists installing OpenWRT on Linksys

[8] *Id.* at para. 46.

[9] *Software Security Requirements for U-NII Devices* (Mar. 18, 2015), Federal Communications Commission, Office of Engineering and Technology, Laboratory Division, 594280 D02 U-NII Device Security v01r02, p. 2.

WiFi routers. Mozilla's own Firefox OS mobile operating system powers devices in over two dozen countries all around the world offered by several different manufacturers.[10]

In some circumstances, open source technologies powering devices with radio capabilities include capacities to modify power levels and the frequency of transmissions. For example, some projects use code from the open source Linux operating system, which includes a wireless configuration tool "iwconfig." This program includes the ability to specify frequency and transmission power settings in communication with a radio device.[11]

Although perhaps not the Commission's intention, it seems very possible that the scope of the proposed rules controlling software modifications would encompass these open source software systems, and would require device manufacturers to go to new lengths to control or prohibit their use.

One of the most significant benefits of open source is in its ability to inspire and enable downstream uses, not envisioned by the original developer, tailored to specific interests and use cases. For example, before its official release, early Firefox OS code bases were actively being ported to the popular 'Raspberry Pi' device platform.[12] The Android Open Source Project produces code for wireless devices that is used both by Google and by downstream vendors in distinct projects.[13]

[10] Firefox OS, Android, Marketplace – Partners, Mozilla, *available at* https://www.mozilla.org/en-US/firefox/partners/.

[11] iwconfig, LinuxCommand.org, *available at* http://www.linuxcommand.org/man_pages/iwconfig8.html.

[12] *Firefox OS for Raspberry Pi*, Raspberry Pi Blog (Aug. 16, 2012), *available at* https://www.raspberrypi.org/blog/firefox-os-for-raspberry-pi/.

[13] *See, e.g.*, Ron Amadeo, "Google's iron grip on Android: Controlling open source by any means necessary," *Ars Technica* (Oct. 21, 2013), *available at* http://arstechnica.com/gadgets/2013/10/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/ (describing the open source core of Android, AOSP, and identifying Amazon's Kindle Fire as built on top of AOSP).

These open source powered advances in mobile technology are inconsistent with a regulatory approach that would impose restrictions on downstream software development through mandatory security mechanisms to prevent modifications.

**Non-harmful modifications should not be barred by restrictions or gatekeepers.**

We recognize the harms that arise from setting power levels and transmission frequencies beyond normal use cases and established limits associated with the use of both licensed and unlicensed spectrum. We also understand the desire to encourage more spectrum reuse, and the value of so doing, by enforcing these restrictions in practice.

But the Commission need not and should not engineer technological barriers into the wireless ecosystem in order to advance these goals. Software security controls that explicitly prevent subsequent software modification risk not only impeding innovation in the context of research and development, but also harming the open source wireless world developers and users enjoy today.

The NPRM offers a better approach: focusing on existing certification compliance requirements, and permitting without re-certification downstream modifications to software that do not cause wireless technology to exceed its legal permitted transmission power and frequency. The Commission can and should continue to enforce its rules against bad actors through post-hoc penalties, regardless of whether the spectrum at issue is licensed or unlicensed. But enforcement must not include prior restrictions that preemptively tie the hands of developers, researchers, and users of technology regardless of whether their actions would violate the terms for spectrum use.

We appreciate the Commission's efforts as well as the complexities in this proceeding, and we look forward to continued collaboration on this issue with the Internet and telecommunications community in order to improve spectrum policy for the future.

Respectfully submitted,

Chris Riley
Head of Public Policy
Mozilla

October 9, 2015